PCI

It's not just for card companies anymore.

ebook

An SC Magazine publication

PCI

PCI standards shook up – and much improved – the security situation for credit card companies. Some think it's time the standard was applied more broadly. Alan Earls reports.

For many companies that process credit and debit cards or retail customers' credit card data, the requirements of the Payment Card Industry Data Security Standard (PCI DSS) are all too familiar. While the standards have not stopped cybercrime, they have provided a baseline for security practices that individual organization have built on. And they are credited with improving security for the industry and for companies using the standard.

That success, and that role as a foundational security standard, leads to the logical question: Should companies that are not required to implement PCI DSS do so anyway in order to try to get the same benefits? Perhaps having a proven tool in place will help provide a starting point for more and better security practices.

OUR EXPERTS: PCI

Jonathan Care, research director for privacy and security, Gartner
Mary Castleton, IT project manager, Davinci Virtual Office Solutions
Michael Kemp, co-founder, Xiphos Research
John Kindervag, vice president and principal analyst, Forrester Research
David Lacey, cybersecurity researcher and consultant
Ryan McElrath, CTO, Americaneagle.com
Dmitry Vyrostkov, chief software architect, DataArt

"PCI compliance is beneficial to a company collecting credit card or private information to make sure their customers or viewers information remains safe," says Mary Castleton, IT project manager at Davinci Virtual Office Solutions, a services company based in Salt Lake City. However, Castleton admits, staying PCI compliant "can be a pain." An e-commerce business, for example, must prepare a lengthy yearly application. Also, the standards are constantly changing and evolving to keep up with technologies, "So there is always the possibility that updates – and sometimes costly updates – have to be done to the server or the website to ensure the site stays compliant," she says.

"I think PCI DSS is hugely valuable," says John Kindervag, vice president and principal analyst at Cambridge, Mass.-based Forrester Research, and a former qualified security assessor (QSA). In his current role, he says it is important to think of PCI as something like a "12-step program." It isn't meant to be bulletproof, but, rather, to address the tendency of each player in the credit card value chain to see security as someone else's problem. "All compliance is the result of a failure of corporate governance," he adds.

PCI does two things: It incentivizes good security practices and it provides better tactical security than other systems. On the other hand, it implements many specific requirements on participants, requirements that often raise howls of protest. "No one likes to be told what do," says Kindervag, "but when you ask people which PCI requirement they think should be omitted they are forced to admit that they are all important."

Latching on to PCI DSS has another benefit, he says. It unlocks security budgets. "It is the only security standard that is the same everywhere in the world, no matter whether you are a big or small entity, everyone has to deal with it the same way," says Kindervag. In other words, it offers a sensible starting point for any security program.

And, he says, it makes sense to apply it across more companies. "I might say, I run a hospital, why do I need PCI. However, if you take credit cards in your cafeteria, you are a credit card merchant, too."

He contrasts PCI with the NIST Cyber

94%

PCI-DSS-compliant companies say compliance improves their relationship with business partners.

Source: Dell

Security Framework, which he dismisses as "compliance by cheerleading." At least with PCI, he explains, there is a clear minimum you must do with basic things, such as password complexity and reset options. "If you take PCI as your baseline and don't go beyond, you will be in compliance and you will have better security," he adds.

Kindervag says he has clients who have worked at PCI-compliant companies and then gone to other businesses not operated under PCI. "Invariably, the security is much worse," he says. "PCI represents a set of robust controls and it was the first datacentric view of security at a time when everything else was network- or device-centric," he notes.

> "...data protection has become the number one job in all data security."
>
> *– John Kindervag, analyst, Forrester Research*

"With EU (European Union) data protection requirements or those in California, data protection has become the number one job in all data security, and PCI taught us how to do it," says Kindervag.

Michael Kemp, co-founder of Xiphos Research, a Birmingham, England-based security consulting firm, agrees that PCI-DSS is a great baseline for those handling or storing card data, but as with so much in IT, it can be repurposed. "The guidelines offered by PCI DSS can be a very useful starting point for improving organizational security, but they are only guidelines, and should only be treated as such," he says.

Kemp warns that blind adherence to a standard is a path that can be fraught with problems, not least of which is that just because your organization, your auditors and your penetration testers implement and test against the standard, it does not mean that attackers will think like you, he explains. Also, security remains only as strong as its weakest link – and that can sometimes be an adherence to an inflexible standard designed to protect cash, not estates.

Furthermore, he notes, PCI has been deficient in a number of key areas historically, "and it is often treated as a tick box exercise by many organizations that seek to apply it." For example, Kemp says in recent years a number of high-profile attacks have occurred against supposedly compliant merchants that apparently adhered to the standard and had even been audited.

"The fault there does not lie with the standard but its application and possibly with those vendors that are doing the bare minimum to achieve compliance," he says.

Kemp says the current DSS has a number of key controls and core requirements for compliance, namely:

- Build and maintain a secure network;
- Protect cardholder data;
- Maintain a vulnerability management program;
- Implement strong access control measures;
- Regularly monitor and test networks; and
- Maintain an information security policy.

"All are relevant to any organization that has security as an organizational driver," he says. Some PCI-DSS requirements are extremely basic, such as demanding the use of firewalls, something that is now nearly universal across all business sectors. "A strong perimeter is necessary for any organization regardless of the data set it holds," says Kemp.

Similarly, allowing the use of default credentials is something no organization should permit. "Presently shodan.io has a list of thousands of devices and databases across the globe that use default vendor-supplied credentials – and attackers, be they legitimate testers or criminals, routinely hope to hit on the magical combination of username: admin and password: admin," he notes.

The PCI standard also mandates encryp-

90%

Percentage of companies where compromised credentials are a major concern for corporate security executives

Source: Rapid7

Case Study: Adopting PCI at a web hosting company

Americaneagle.com has developed and hosted websites since 1995. In 2006, the company's ecommerce prospects and customers began asking about PCI compliance and what Americaneagle.com was doing in that regard. The owners of the company asked Ryan McElrath, the Fort Lauderdale, Fla.-based company's CTO, to find out what it would take to meet PCI compliance requirements.

"At the time, I wasn't enthused about this as it looked like a major undertaking for us," says McElrath. "We felt like we were already doing a lot for our customers' website security and this was going to be a lot of extra work to document our policies and processes, keep them updated, and so on."

Ryan McElrath, CTO, Americaneagle.com

A referral to the auditing company Fortrex helped provide Americaneagle.com with a "gap analysis" to determine what would be required to pass a full PCI service provider audit successfully. "This was very helpful and we came out of that with a to-do list with a goal of having Fortrex audit us in the fall of 2007," he says. At the time, the company was in the process of opening up new data center space and they configured that to meet PCI compliance from the start. In the summer of 2007, the company started migrating hundreds of ecommerce sites to the new data center space and then had that space audited (successfully) in the fall of 2007. "We were an early adopter of PCI as, at that time, we were one of the first 10 data centers in the world to achieve PCI compliance in the area of managed hosting," he says

Passing the audit was a huge step, but McElrath says the company remained skeptical about PCI compliance and wanted to minimize the time spent on it. "We were planning on creating two segments on our network – one that had to meet PCI compliance standards [namely for ecommerce sites and any other sites that handle credit card information] and one that didn't need to meet PCI compliance standards," McElrath explains. "We started in that direction and then changed our minds. We thought it was going to be too cumbersome to handle servers and sites in two different manners," he says. More importantly, we started to see that the PCI security standards did help make sites more secure, he says. "We wanted to bring that level of security to all of our sites, not just ones that handled credit card information," so instead of running from the PCI standards, the company did a 180-degree turn and embraced them.

"If we had not started securing all of our sites this way, then we most likely would have suffered multiple security breaches over the years, which would have been damaging to our customers and to our reputation as a web hosting provider," says McElrath. Americaneagle.com has been successfully audited as a PCI service provider since 2007.

"To give you an idea of how much things have changed security-wise over that period, the first detailed "Report on Compliance (ROC)" document created by our auditor back in 2007 was 80 pages. The 2015 version of this is now over 400 pages – five times larger in nine years," notes McElrath.

PCI compliance might also have helped the company to expand. In the fall of 2009, Americaneagle.com won the opportunity to be involved in building and hosting website projects related to the White House – conforming to the *Federal Information Security Management Act* (*FISMA*) and top secret level clearance requirements. "This is noteworthy because it had nothing to do with PCI security or credit cards, but our work with PCI compliance helped us meet the

0%

Not a single company in the past decade has been found to be PCI compliant at the time of a breach.

Source: Verizon

tion (for cardholder data) across public networks and this makes sense for any organization that handles sensitive data of any sort, whether it is medical records, payroll information or even communications with customers. Likewise, it certainly makes sense to encrypt anything which could be considered sensitive data, he says.

"The use of anti-virus is also mandated by the standard, and as the growing tide of sophisticated malware shows, having protections in place can save organizations a lot of heartache and technical overhead for a small financial cost," says Kemp. Maintaining secure systems and applications, as defined by the standard, and assigning unique identifiers is also essential for any organization that cares about security. Attackers crave insecure systems, says Kemp, and if those systems don't attribute actions to users, separating legitimate actions from illegitimate ones can be a major headache for organizations.

> "The PCI DSS outlines a great list of current and actionable security best practices..."
>
> *– Dmitry Vyrostkov, chief software architect, DataArt*

PCI DSS allows organizations that handle card data to secure their crown jewels (namely card data), but every organization has crown jewels of one kind or another, he notes. "This can be as varied as details about intellectual property, staff, physical premises, stock control, payroll, commercial relationships and a whole host of others things," he says. It applies to any key data.

It is also worth noting that attackers know that any "private" data has financial and logistical value. Organizations should recognize this too, whether or not such data is financial. As an example, let's say you run a florist that serves film stars. The addresses of Hollywood A-listers (and those to whom they are sending flowers) might be a lot more valuable to a suitably corrupt attacker than the credit card details of a teacher in Ohio, which are worth a negligible amount on the black market. That is why applying a strong security baseline for any organization is not only useful, but in an age of daily increasing threats and risks, a necessity, Kemp adds.

Adoption advice

"The PCI DSS outlines a great list of current and actionable security best practices that all IT companies should consider while evaluating their security," says Dmitry Vyrostkov, chief software architect at DataArt, a New York-based technology consulting firm. For instance, he notes, the "Cardholder Data" term used widely in the standard could be adopted to represent any sensitive information with which a company operates. "Simply browsing through the list of PCI requirements will give a CIO, CSO or CTO a lot of ideas for improving a company's security perimeter and internal processes," he says. Businesses should employ a reasonable prioritization based on the list of current risks, company profile and operations, he adds.

PCI DSS contains many standards of good security practice that are applicable outside of the card processing environment, agrees Jonathan Care, research director for privacy and security at Stamford, Conn.-based Gartner. These include familiar things such as effective patch management and regular testing.

"One of the challenges of PCI DSS is that by design it is prescriptive," says Care. That means the scope is defined (cardholder data), the data classification is set, and there is no room for risk assessment of controls – reflective of the original purposes of PCI DSS, which was to establish a baseline security standard in a wide variety of organizations with patchy records of securing cardholder data.

According to Care, it is notable that in recent breaches, cardholder data loss has been reduced, while unprotected data, such as bank

28.6%

Companies found to be fully compliant less than one year after a successful PCI validation.

Source: Verizon

account details, have continued to be exposed. However, Gartner's recommendation is to reduce to an absolute minimum the cardholder data held in the enterprise, and use techniques, such as tokenization and point-to-point encryption, to reduce the need to re-engineer infrastructure and application components to meet the requirements of PCI DSS.

This is an indicator that enterprises are not using the techniques of PCI DSS outside of the strict scope required of cardholder data processing, storage or transmission, he says. However, he notes, employing good security practices in an enterprise-wide context outside of the narrow scope of PCI DSS is likely to improve the organizational security posture and reduce the impact and incidence of data breaches.

Jonathan Care, research director for privacy and security, Gartner

Within the scope of PCI DSS, it appears unfortunate that many qualified security assessors (PCI consultants) are not giving their clients advice that embraces holistic security across the enterprise, says Care. It is also unfortunate that many QSAs are still stuck in the "rip, replace, assess" loop that will require constant change as PCI DSS requirements evolve. Also, many focus too much on infrastructure components and not on web application security, one of the areas where card fraud is rampant.

Gartner's recommendation is to put protective controls in place to safeguard sensitive data and infrastructure and application level, and to ensure that measures are in place to detect the inevitable attacks from all sources, he says. "With a clear appreciation that there will be a determined and resourced attacker who will evade controls and detection, a well thought out incident response process is a vital component of a mature security posture," Care says.

"If you find PCI DSS challenging, it's because you don't have enough security," David Lacey says flatly. He is a cybersecurity researcher and consultant, author of ISACA's *A Practical Guide to the Payment Card Industry Data Security Standard (PCI DSS)*. "PCI is expensive, but not as expensive as a major data breach," he says. It might seem more stringent than other standards, but that's because it's rigorously enforced and updated. "PCI DSS is a necessary standard to prevent professional thefts of data," he notes.

If you have customer data of interest to organized crime, you are a target. Last October's TalkTalk hack compromised customer bank details, but not their payment cards. For Gartner's Care, that is proof that PCI DSS works. "That should be enough to persuade other retailers to extend their encryption to other customer data," he says.

Simply trying to skate by on the minimum requirements once a year to pass an audit is not the right way to do PCI, says Ryan McElrath, CTO at Americaneagle.com, a Fort Lauderdale, Fla.-based web hosting company that adopted PCI almost a decade ago. "While we have created dozens of documents and hundreds of pages about our policies and processes, our goal is that we rarely have to look at them on a day-to-day basis," he explains. This is because Americaneagle.com has built a company intranet that has the change management and approval process built into it. In addition, his company:

- Has monitoring in place to watch various requirements of PCI;
- Has daily PCI-related tasks assigned to various personnel within the hosting department;
- Is subscribed to numerous security news bulletins and vendor bulletins;
- Conducts internal quarterly review meetings to assess progress on various tasks;
- Conducts training meetings throughout the year; and
- Continually looks for ways to improve.

80%

Four of five companies fail at interim PCI complicance assessments.

Source: Verizon

When a story about a major breach comes out there is a tendency for people to have a knee-jerk reaction and bash the PCI requirements and say, "Well, that company was PCI-compliant and it still didn't protect them," says McElrath. Usually, though, he says the real story is that company that suffered the breach wasn't actually following the PCI requirements at the time of the breach. Those are the instances where companies view PCI compliance simply as an annual event around the audit rather than having PCI requirements embedded into their daily practices. "We feel PCI has been very helpful for us because of the approach we've taken toward it," he adds.

PCI DSS has raised the bar of expectation and encouraged the development of better security products, says Lacey. For example, "We can all benefit from encryption, asset management, network segmentation, tokenization and secure managed file transfer," he adds

But Forrester's Kindervag advises steering clear of "scare" stories about the challenges of PCI, which he insists are overblown. "If you have to do it, just do it and quit complaining," he says. "You have to understand what you are trying to accomplish and take a positive view. There is nothing in PCI that you shouldn't be doing anyway." ■

For more information about ebooks from SC Magazine, please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

PCI

0.077

seconds: Time it takes to crack the password "bigmac."

Source: PCI Council